JOURNAL OF CYBER COVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 Article 7

Evaluating the Legal Framework for Combating Cyber Crime in India

Suhani Sharma

Amity University Rajasthan

Recommended Citation:

Sharma (2026) "Evaluating the Legal Framework for Combating Cyber Crime in India" Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 7. (DOI)

ABSTRACT

India's digital growth over the past two decades has been remarkable, with the growth in people coming online, doing more transactions digitally and what not. This showcases that everyday life has moved into cyberspace but this shift has also opened the door to a growing and increasing wave of cybercrime. This paper discusses whether India's existing laws are actually equipped to deal with this reality. With the focus on three key legislations: The Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023. While these laws have modernized India's legal response to digital threats, serious gaps are present between what the law says and what actually happens on the ground. The paper also mentions the obstacles that weaken the enforcement which include that tools like Tor and VPNs, the jurisdictional dead ends that arise from the borderless nature of the internet, the paper also argues that current penalties are not severe enough to stop offenders. Based on these, it suggests a move toward standardized forensic protocols, multilateral international cooperation, and dedicated cyber courts. The central argument is straightforward: India has the legislative intent, but needs to close the gap between that intent and actual implementation if it wants to protect its citizens in this age of digital crimes.

KEYWORDS

Cybercrime, Information Technology Act, Cyber law, Digital security, Cyber fraud, India

INTRODUCTION

Modern society is witnessing an unprecedented rise in the digital world. Every activity that we carry out, from doing e-commerce to communicating amongst friends, is now done via the internet. While this surge in internet usage has drawn positive outcomes in terms of interconnectivity and better opportunities, it also has uninvited consequences. More and more people are being exposed to crime through virtual channels. When looking at depth into this darker side, cybercrime emerges as a major concern. Cybercrime can be defined "as *an unlawful act in which a computer, communication device, or computer network is used to commit or facilitate the commission of a crime."*[1]

The most recent annual report, as of March 2026, released by the "National Crime Records Bureau (NCRB), titled Crime in India 2023, illustrated a 31.2 percent rise in cybercrime cases.More than 86,420 incidents related to cyber offences were reported, marking a 31.2 percent increase from the previous year, with Karnataka alone accounting for 21,889 cases highlighting the concentration of cyber fraud in major technological hubs.[2] With the increasingly unavoidable inclusion of digital ecosystems into our lives, cybercrime has become a major concern. This report's data showed a stark growth of cybercrimes in recent years. It's important to understand that cybercrime is not a single entity; it possesses many branches in the virtual world such as:

1. Hacking and Unauthorized Access: Gaining illegal entry into computer systems, networks, or digital accounts without authorization, often with the intent to steal data or cause damage.

[1] National Cyber Crime Reporting Portal, Ministry of Home Affs., Gov't of India.

[2] National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs, Dec. 2025).

2. Ransomware Attacks: A type of malware that encrypts a victim's data and demands payment in exchange for restoring access. Critical sectors such as hospitals and government institutions are frequently targeted.
3. Online Financial Fraud: Includes credit card fraud, UPI scams, fraudulent banking websites, and unauthorized financial transactions designed to steal money from victims.
4. Malware and Virus Attacks: The deployment of malicious software such as Trojans, spyware, and worms to damage systems or secretly collect sensitive information.

With the continued growth of this digital ecosystem in our lives, newer and more sophisticated forms of cybercrime are also emerging from time to time.

In response to these threats, the government has taken steps to regulate digital exploitation and to implement safeguarding legal measures. Various laws have been introduced and strengthened to define cyber offences clearly and prescribe strict penalties. These legal statutes aim to uphold national security while protecting citizens from fraudulent and unlawful online activities.

This research paper analyses the current legal framework addressing digital crimes in India. It aims to find the most glaring gaps in existing laws and suggest reforms that can potentially help India's response to cyber threats towards its citizens. The research tries to inspect the effectiveness of contemporary cyber laws. It also tries to study how courts have interpreted these laws over time, highlighting where these frameworks fit and where they don't. The goal is to illustrate these weaknesses and pose practical reforms that can be implemented to facilitate a more robust cybercrime response by the Indian government.

LITERATURE REVIEW

Many scholars have researched the effectiveness of India's legal frameworks to fight against cyber threats exacerbated due to the ever-increasing involvement of people with the digital world. According to Ahmad Muhammad Tahir (2025), the Information Technology Act is a crucial part of the legal framework with regard to the digital realm; however, notable gaps exist in addressing modern age threats such as AI-driven attacks and massive data breaches,

underscoring the need for a more comprehensive cybersecurity law. Tahir addressed that while India is experiencing rapid digital transformation, it is also confronted with an increasing surge of complicated threats, including ransomware and deep fake-based impersonation, which are not effectively covered by the current legal statutes.[3] N.S. Nappinai highlighted this interconnected landscape as a state of "Cyber Pangea," where online fraud operates across jurisdictions, blurring the boundaries between traditional territorial legal systems and established jurisdictional frameworks.[4] Additionally, Monica Madaan and Arryan Mohanty (2025) observed that the inequitable nature of India's socio-economic status is exacerbating this vulnerability, as a significant percentage of the population still lacks basic digital literacy, positioning them as "prime targets" for online identity-related frauds.[5]

Additionally, It was observed by Pallavi Kapila (2020), that the Act was originally conceived to provide legal recognition for electronic commerce and digital signatures, heavily influenced by the UNCITRAL Model Law.[6] Legal experts like Pavan Duggal argued that the 2008 amendments were transformative, as they brought the Act's penal scope to include more specific offences such as identity theft under Section 66C and cheating by personation under Section 66D.Subsequent research by Bhangla and Tuli (2021) observed a significant rise in identity theft across social networking platforms like Facebook, noting that Sections 66C and 66D had proven instrumental in safeguarding digital identities and imposing accountability for fraudulent profiles.[7] Despite these advancements, Adv. Jyoti Akshay Murhe noted a persistent "procedural lag," arguing that the Act is heavily focused on digital certification and commercial transactions, often lacking the precise definitions required to prosecute evolving computer-related crimes like "Frankenstein fraud".[8]

---

[3] Ahmad Muhammad Tahir, The Efficacy of the Information Technology Act, 2000 in Addressing Emerging Cyber Threats in India, 14 Int'l J. Sci. & Res. 1692 (2025).
[4] N. S. Nappinai, *Cybercrimes and the Law*, Jharkhand Jud. Acad. (2025).
[5] Monica Madaan & Arryan Mohanty, *Identity Theft in the Digital Age: Legal Challenges and the Evolving Role of Law Enforcement in India*, 4 Cyber L. Rep. 44 (2025).
[6] Pallavi Kapila, *Cyber Crimes and Cyber Laws in India: An Overview*, *in* Contemporary Issues and Challenges in the Society 36 (New Era International Imprint ed., 2020).
[7] A. Bhangla & J. Tuli, *Identity Theft and Impersonation in Social Media*, 8 Int'l J. Innovative Res. Tech. (2021).

[8] Adv. Jyoti Akshay Murhe, *Critical Appraisal of Section 66 of Information Technology Act 2000*, Int'l J. L. & Rsch. Analysis (2023).

Research regarding implementation of cyber laws indicates a critical gap between legal theory and on-ground reality. Scholars pointed out that the borderless nature of cybercrime complicates issues of jurisdiction and evidence retrieval, particularly when data is stored on foreign servers like those maintained by Meta. Research by Monica Madaan and Arryan Mohanty suggested that Indian law enforcement is often confronted with issues related to limited resources, a lack of specialized forensic infrastructure, and an evasive digital literacy gap among both the public and the police. Furthermore, the procedural complexities involved in complying with evidentiary standards under Section 65B of the Indian Evidence Act, 1872, which requires strict certification for the admissibility of electronic records often impede the successful prosecution of identity related crimes. Jan and Bashir (2025) emphasized that these evidentiary issues are particularly prevalent in the era of deep fakes, where separating genuine and morphed digital footprints has become a "forensic nightmare".Their research further highlights how AI-enabled impersonation techniques are evolving faster than statutory definitions, creating enforcement gaps in identity-based cyber offences.This view is also supported by leading legal commentators such as Pavan Duggal and Vakul Sharma, who argue that the statutory framework has not evolved proportionately with emerging technological risks.[9][10]

Scholars recommend a multi-layered approach that includes criminal law with effective data protection protocols. Madaan and Mohanty noted that the enactment of the Digital Personal Data Protection (DPDP) Act, 2023 proved to be a significant push towards a preventive regulatory framework that prioritized accountability of "data fiduciaries" rather than circumventing around punishing post-offence. Furthermore, N.S. Nappinai emphasized the necessity for a dynamic legislative framework that can address the unique challenges posed by the rise in Artificial Intelligence, arguing that current statutes must be synchronous with the Bharatiya Nyaya Sanhita (BNS), 2023, to avoid overlapping definitions and legal gray areas. Saima Jan and Anna Bashir (2025) also argued for a "compelling need" for dedicated Deep fake Prevention and Regulation Act to charter clear legal boundaries and consequences for malicious digital activities.[11] Recommendations for the future also include strengthening international cooperation, focusing

[9] Pavan Duggal, Cyber Law: An Exhaustive Section-wise Commentary (3d ed. 2024)
[10] Vakul Sharma, Information Technology Law and Practice (9th ed. 2025).
[11] Saima Jan & Anna Bashir, *Legal Frameworks on AI-Enabled Identity Theft: Challenges and Recommendations*, 30 J. Intel. Prop. Rts. (2025).

efforts on increasing cyber forensic training, and creating a cohesive national cybersecurity strategy that prioritizes the constitutional right to privacy under the Puttaswamy precedent with rigorous enforcement requirements.

METHODOLOGY

This research is qualitative in nature and relies majorly on secondary sources. The aim is to get an understanding of how India's legal framework deals with cybercrime not just what the law says on paper, but how it actually functions and what gaps are present in between all this.

The primary sources used in this study were existing laws and statutory provisions. The three legislations that formed the backbone of this analysis are the Information Technology Act, 2000 (as amended in 2008), the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023. Reading and interpreting these statutes directly was essential to understanding what the law actually covers and where it leaves gaps.

Other than that the research is done by the help of academic literature, legal commentaries, government reports, and policy discussions published in journals and books.

The research also looked closely at landmark judgements like Shreya Singhal v. Union of India and Justice K.S. Puttaswamy v. Union of India to understand how courts have interpreted these laws and shaped their application over time. Case law is where theory meets practical reality, and decisions often reveal things about a law's strengths and weaknesses that the text of the statute alone cannot.

Finally, the study paid close attention to the challenges that previous researchers have identified like jurisdictional limitations, problems with admissibility of digital evidence, and gaps in enforcement capacity. The goal throughout was not just to describe what the law says, but to honestly assess whether it is working and if not, why not.

LEGAL FRAMEWORK ANALYSIS

This section evaluates the legal framework India has built to address the various challenges related to the digital world. This covers The Information Technology Act of 2000 and its amendments, The reforms that came with the introduction of The Bharatiya Nyaya Sanhita , The Bharatiya Sakshya Adhiniyam in 2023 and how introduction of The Digital Personal Data Protection Act 2023 brought reforms for individual rights in the digital age.

The Information Technology Act, 2000[12]

When the IT Act was enacted in 2000, the internet in India was still in its starting phase. Broadband was not known by many, smartphones did not exist, and the idea of online fraud at the scale we see today was something no one had thought of. The purpose of the Act at that time was to give legal recognition to electronic commerce and digital records, so that online contracts and digital signatures could be treated the same way as the physical ones.

The 2008 Amendment Act was the turning point as it introduced a set of criminal provisions that specifically targeted computer related offences.[13]

The philosophical idea of the IT Act was to bring technological neutrality which means that the law should not be tied to any one platform or device, but should apply broadly to the digital world regardless of the medium. Some of its important features are:

- It provides a safe framework for intermediaries which means that the internet platforms are not automatically held liable for content posted by their users, as long as they observe prescribed due diligence standards.
- It has moved from the old idea that crime can only be done physically, to now viewing manipulation of data, unauthorized system access, and breach of digital trust also as crime.
- It recognizes both civil (Section 43) and criminal offences (Section 66 onwards), which gives courts flexibility while giving judgements.

Key Provisions

[12] Information Technology Act, No. 21 of 2000, 66C (India).

[13] Information Technology (Amendment) Act, No. 10 of 2009 (India).

Section 66C

Section 66C was introduced to address the fraudulent use of someone else's digital credentials like their passwords, electronic signatures, biometric data, or any other unique identification feature. In the digital world, your identity is essential for your login details, and Section 66C treats the misappropriation of those details as a serious criminal act. The key elements are:

- The accused acted with fraudulent or dishonest intent.
- They used someone else's electronic identity like a password, digital signature, or biometric data without any authorization.
- The actual owner never consented to this use.

The maximum punishment is three years of imprisonment and a fine of up to one lakh rupees.

Section 66D

Section 66D talks about the act of cheating someone by pretending to be another person through a computer or any device. This is directly relevant to phishing scams and social engineering attacks. Key points about this provision:

- It covers situations where a person poses as a bank representative, government officer, or any known contact to manipulate a person to hand over money or sensitive information.
- The punishment is up to three years in prison and a one lakh rupee fine.

Section 66E

Section 66E deals with the intentional capturing, publishing, or transmitting of images of a person's private areas without their consent and in circumstances where they had expectation of privacy. Some important features of this are:

- This section is gender neutral, reflecting that privacy and bodily dignity are fundamental rights regardless of gender.
- The basis of the offence is the reasonable expectation of privacy like a bedroom, a changing room, a private bathroom are spaces where a person should be able to exist without fear of being secretly recorded.

- The maximum punishment is three years of imprisonment and a fine of up to two lakh rupees.

The Bharatiya Nyaya Sanhita, 2023[14]

On July 1, 2024, Indian Penal Code 1860 was replaced by the Bharatiya Nyaya Sanhita 2023. The BNS was not just a replacement of IPC but it was an effort to modernize criminal laws by integrating them with the digital world. Some of the significant changes were:

- The definition of a "document" now includes electronic and digital records as well, removing the ambiguity about whether digital files can be a subject of offences like forgery or criminal breach of trust.
- Section 113 of the BNS introduced a new category of terrorist acts that covers attacks on computer resources and digital data that recognizes that cyberattacks on essential systems can be acts of terrorism, not just property crimes.

- Section 77 replaced Section 354D which talked about stalking, now electronic stalking and the psychological harm it causes are also considered.
- Section 71 replaced Section 354C which talks about voyeurism, now its definition includes AI-generated images and deep fakes.

The Bharatiya Sakshya Adhiniyam, 2023[15]

The Indian Evidence Act of 1872 was replaced by the Bharatiya Sakshya Adhiniyam 2023. Several meaningful updates which took place were:

- A certificate must accompany the electronic record when it is produced in court. It must identify the electronic record and the device used to produce it. It should be signed by the person in charge of the computer or device.

[14] Bharatiya Nyaya Sanhita, No. 45 of 2023 (India).

[15] Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India).

- It mandates the inclusion of a hash value which is a unique mathematical fingerprint of the digital file which provides a verifiable way to confirm that the data has not been altered between collection and trial.
- The definition of "computer" now covers smartphones and other devices, which has removed the gap that was in the old frameworks.

The Digital Personal Data Protection Act, 2023[16]

The DPDP Act states that personal data belongs to the person about whom it is and anyone who collects or uses that data has obligations toward that person.

The Act mentions a relationship between the Data Principal (the individual whose data is collected) and the Data Fiduciary (the organization doing the collecting). The principle in this is the consent that the personal data can only be processed for a lawful purpose, and only with informed, unambiguous consent.

Rights of the Individual

Under the DPDP Act, individuals have real, actionable rights over their data like:

- They can request a summary of what data an organization holds about them and ask for corrections to be made.
- Once the purpose for which their data was collected is fulfilled, they can demand that their data be deleted.
- Complaints can be filed in the Data Protection Board if they feel their rights have been violated.
- Individuals can withdraw their consent at any time they want, after which the data has to be erased.

[16] Digital Personal Data Protection Act, No. 22 of 2023 (India).

The Act has devoted specific attention to protecting children like:

- Organizations are prohibited from tracking minors or directing targeted advertising at them.
- The government can classify certain organizations as Significant Data Fiduciaries; they will be the entities handling large volumes of sensitive data and subject them to heightened compliance requirements, including mandatory audits and the appointment of a dedicated Data Protection Officer.
- Failure to implement reasonable security measures that result in a data breach can attract a fine of up to 250 crore rupees per instance.
- Violations of obligations specifically toward children carry penalties of up to 200 crore rupees.
- Mandatory breach notification to both the Data Protection Board and the affected individuals is required in all cases of a data breach.

CASE LAWS

The power of a legal framework is as strong as how courts interpret it and apply it. In the context of the cyber world, judicial decisions hold great significance in dictating what the law actually means, what it can do, where it falls short and how it can evolve. The following cases, showcase a complete picture of how Indian courts have interacted with cybercrime laws over the past decade.

1.*CBI v. Arif Azim (Sony Sambandh Case)*

This case is regarded as India's first conviction involving phishing-related offences, where the accused used stolen credit card details for fraudulent transactions. The court applied Sections 418, 419, and 420 IPC.[17]

2. *State of Tamil Nadu v. Suhas Katti (2004)*[18]

[17] CBI v. Arif Azim (Sony Sambandh Case), C.C. No. 5/2003 (Delhi Dist. Ct.).
[18] State of Tamil Nadu v. Suhas Katti, C.C. No. 4680/2004 (Egmore C.M.M. Ct. 2004).

Facts and Issue

In this case, the accused posted defamatory and obscene messages about a divorced woman across various internet message groups, which led to her receiving harassing and uninvited phone calls. The legal question before the court was whether the Information Technology Act, 2000 which had recently come into force, could be effectively used to prosecute online obscenity and digital harassment under Section 67.

Court's Reasoning

The court convicted the accused, and reached the conclusion that the entire trial was completed within seven months, which was unusually swift for the Indian judicial system. The conviction was done on witness testimonies and basic electronic records submitted by the prosecution. There was no complex forensic procedure involved, the evidence was relatively straightforward, and the court found it sufficient.

Relevance to the Study

This case holds a special place in Indian legal history as the first successful cybercrime conviction under the IT Act. It was a proof that the framework, at least for basic cases, was workable. Law enforcement could investigate, gather evidence, and secure a conviction within a reasonable timeframe. It played an important role at a time when many were skeptical about the new legislation.

3. Shreya Singhal v. Union of India (2015)[19]

Facts and Issue

This case started from petitions challenging the constitutional validity of Section 66A of the IT Act, which made it a criminal offence to send messages that were deemed "offensive" or likely to cause "annoyance" or "inconvenience." The main issue was whether Section 66A violated the

[19] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

fundamental right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution.

Court's Reasoning

The Supreme Court struck down Section 66A entirely, stating that the provision was vague and overly broad. The terms used like "offensive," "annoying," "inconvenient" were too subjective and undefined, which meant that the law could be applied against any kind of speech without any clear limiting principle. The Court held that this created a friction on free expression, discouraging people from speaking freely online out of fear of arbitrary prosecution.

Beyond Section 66A, the Court also significantly reinterpreted Section 79, which deals with intermediary liability. It ruled that intermediary platforms like social media websites are only obligated to take down content when directed to do so by a court or a competent government authority, and not merely on the basis of private complaints. This was a meaningful shift in how online platforms were expected to operate.

Relevance to the Study

This case is one of the most significant digital rights judgments in India. By striking down Section 66A, the Court sent a clear message that cybercrime legislation cannot be so broad that it hinders the dignity of freedom of speech.

4. Anvar P.V. v. P.K. Basheer (2014)[20]

Facts and Issue

This case originated from an election dispute in Kerala, where one party sought to admit CDs containing secondary electronic records as evidence. The question before the Supreme Court was: what is the legally correct method for admitting electronic evidence under the Indian Evidence Act, 1872?

Mainly, the issue concerned was whether a certificate under Section 65B (4) of the Evidence Act is mandatory for electronic records to be admissible.

[20] Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).

Court's Reasoning

The Supreme Court held that electronic records can only be admitted as documentary evidence if accompanied by a certificate under Section 65B(4). This certificate essentially functions as an authentication mechanism; it must be issued by a responsible person in charge of the device or system that generated the record. Without this certificate, the electronic record simply cannot be seen as evidence, regardless of how relevant or genuine it may actually be.

Relevance to the Study

This judgment sits at the heart of one of the most persistent practical problems in cybercrime prosecution in India. The judiciary's intention was to get authentication certificates which meant to ensure that digital evidence is genuine and has not been tampered with, which directly addresses the fragility problem discussed earlier in this paper.

This position was reaffirmed in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 S.C.R. 180, where the Supreme Court clarified that the certificate requirement is mandatory.[21]

5. Justice K.S. Puttaswamy v. Union of India (2017)[22]

Facts and Issue

This case began as a challenge to the Aadhaar biometric identification system, but the questions it raised quickly expanded to something far more fundamental. A nine-judge Constitutional Bench of the Supreme Court was formed and was asked to determine whether the Right to Privacy is a fundamental right under the Indian Constitution, a question that had been a point of contention for a long time.

Court's Reasoning

The bench unanimously held that the right to privacy is indeed a fundamental right, forming an important part of the right to life and personal liberty under Article 21. The Court also

[21] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.R. 180 (India).

[22] Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).

recognized the concept of informational privacy which means that a person's right to control how their personal data is collected, stored, and used.

Relevance to the Study

This is arguably the most significant judgment, because it established the constitution's foundation on which all modern digital rights in India are based. Its legacy includes the Digital Personal Data Protection (DPDP) Act, 2023, which represents India's most serious attempt yet for a comprehensive data protection regime.

CHALLENGES

Cybercrime laws are difficult to put into practice because the features that make the internet such a powerful tool like its openness, its borderless nature, its speed are the things that make it so hard to control. There are various challenges across this.[23] The major obstacles that lawmakers and enforcement agencies continue to face are:

1. One of the biggest issues with the enforcement of cybercrimes is that the internet does not reveal the identity of who you are. Unlike the physical world, where a person committing a crime leaves trace, fingerprints, witnesses, CCTV footage behind. In the online world, identities can be concealed unlike the physical one. Cybercriminals use tools like Tor (The Onion Router) and Psiphon to mask their IP addresses. These tools can pass a person's device with multiple servers spread across different countries and make it almost impossible to trace their activity to a single source. By the time investigators follow the digital trail, it has passed through so many hands and jurisdictions that it has gotten out of their hands.

2. Traditionally criminal law cases are based on jurisdiction. Suppose a court in Delhi has authority over what happens in Delhi. A law passed in India is applied in India.

[23] Ajit Kumar et al., Cyber Law and Digital Governance in India: Challenges and Emerging Trends, 1 Int'l J. Advanced Digital Sys. & Multidisciplinary Stud. (IJADSMS) 53 (2026).

Cybercrime does not apply to a specific jurisdiction. A cybercriminal sitting in Eastern Europe can target a bank in Mumbai, cause real financial damage to real people, and face no immediate legal consequences because the country that suffered the harm has no jurisdiction over someone who was never physically present in its borders. Even if it is identified who did it, local courts often lack what is called "jurisdiction in personam" that is, the legal authority to try a person who is elsewhere. This gap cannot be fixed alone by territorial authority. Even if a country passes the strictest cybercrime laws possible in the world, still if the offender is abroad, those laws simply cannot reach them.

3. In the rare cases where a cybercriminal is identified and located in a foreign country, and the government has to actually bring them to trial is not at all an easy task. This is the process of extradition “formally requesting another country to hand over a suspect”. It is slow, expensive, and comes with many obstacles. Under international law, there is no obligation of one country to hand over a criminal to another. Occurrence of extradition depends on whether a bilateral treaty exists between the two countries in question. And even when such a treaty does exist, extradition can still be refused on the basis of what is called the dual criminality rule meaning the act must be recognized as a crime in both countries. Given that cybercrime laws vary wildly across jurisdictions; this is not always a given.

4. In a crime, evidence tends to be physical either a weapon, a document or a witness. In cybercrime, the evidence is almost entirely digital, and that creates a very specific set of problems. Digital evidence is fragile. It can be altered, deleted, or corrupted sometimes deliberately or by accident. A small wrong step during the process of collection or analysis can compromise the evidence entirely. Indian courts view digital evidence with some degree of skepticism, given that it is far easier to fabricate or tamper with compared to physical proof.
5. Given that the legal framework was perfect, enforcement would still struggle because of the gaps within the institutions which are responsible for carrying it out. Many cybercrime incidents simply go unreported. Corporate victims in particular often hesitate

to disclose breaches, fearing the damage of their reputation that comes with admitting that they were compromised.

6. Cyber forensics is an expensive field. Hiring of experts, using forensic tools, and engaging with specialized legal counsel are very important but costly parts of cyber investigation, especially for smaller organizations or state agencies working under limited budgets. Many cases get dropped because of the high costs even while having full proof evidence.
7. The punishment in many countries including India are too mild which cancels the fear for offenders. The maximum sentence for a serious cyberattack is five years, and actual convictions remain rare, the reason for a technically skilled criminal to feel that the risk of getting caught outweighs the reward.

These issues are consistently highlighted in recent academic discussions on cyber law enforcement in India.[24]

RECOMMENDATIONS

The various challenges that make the enforcement of cybercrime laws difficult, have made it quite clear that the existing legal framework in India is not doing enough. The Information Technology Act, 2000 was the starting point, but the digital scenario of the 2000s and today is very different. So to overcome these challenges various reforms are needed. This section suggests some practical reforms that can make a difference.

1.Given that digital evidence is still viewed with a lot of suspicion by Indian courts, which honestly is not entirely unreasonable as digital data can be altered, deleted, or planted. India needs a standardized protocol for collecting digital evidence. One concrete step would be that the investigators would have to apply cryptographic hashing the moment they seize a digital device or access data at a crime scene. This creates a kind of digital fingerprint of the evidence that can

[24] Ajit Kumar et al., Cyber Law and Digital Governance in India, 1 Int'l J. Advanced Digital Sys. & Multidisciplinary Stud. 53 (2026)

prove it has not been tampered. In the current scenario, this is done but is inconsistent and the inconsistency is one of the reasons cases fall apart in court.

2. Cyber forensic investigations are expensive, and most state agencies and smaller organizations simply cannot afford the kind of equipment and expertise required. A solution for this would be to establish government funded cyber forensic laboratories across the country. This way lack of finances will not be a hindrance in solving a valid case.

3. The jurisdictional problem of cases is the most complex problem in this field because it requires cooperation from other countries which is not an easy thing to achieve. But to get a solution for this to an extent, India should more actively enter in multilateral cybercrime treaties. The Budapest Convention on Cybercrime, for instance, has been adopted by a significant number of countries and provides a shared framework for cross-border investigation and prosecution. India has a slow pace in formally aligning with such international treaties and this gap has real consequences. Similarly, the recently adopted UN Cybercrime Treaty is also a great opportunity for countries.

4. A way to reduce the obstacle of extradition is the dual criminality rule: which requires that an act be a crime in both countries for extradition to happen is to bring India's domestic cybercrime definitions closer to international standards. If Indian law defines offences in a way that are similar to what other countries recognize, fewer extradition requests will be refused on this ground.

5. The punishments for cybercrime under Indian law are mild enough that they barely register as a real risk for someone who is skilled and reasonably careful about their activity. The IT Act 2000and the Bharatiya Nyaya Sanhita (BNS)2023 need to be revisited with this in mind. Penalties should be based on the scale and intent of the offence. Large scale, financially motivated cybercrime should arguably be classified and prosecuted as organized crime, with sentences that reflect that seriousness. Beyond imprisonment, financial penalties and asset freezing should be made a standard part of sentencing.

These reforms point toward a broader shift in how India approaches cybercrime from a largely reactive system that chases evidence after the fact, to a more straightforward one that discourages offences, makes prosecution more reasonable, and builds the international partnerships needed to reach criminals who operate from beyond its borders. None of these changes are simple or quick, but they are necessary if the legal framework is to keep pace with the upcoming developments and threat it is meant to address.

CONCLUSION

The growth in the digital world has created amazing opportunities for economic growth and global connectivity; on the other hand, it has revealed weaknesses that traditional legal systems were not ready to handle. Cyber-attacks, happening in a complex technological environment, are not limited by international borders. To block these malicious activities, there's a clear need for a strong legal framework. India has witnessed significant progress in this area with the enforcement of The Information Technology Act 2000,[25] The Digital Personal Data Protection Act 2023[26], and The Bharatiya Nyaya Sanhita 2023.[27] The government is trying to modernize its legal system. These laws define, categorize, and prosecute digital crimes, ranging from data breaches to financial fraud.

Due to some obstacles, it's still difficult to investigate and prosecute cybercrime. These attacks frequently happen across borders which cause serious issues in law enforcement due to complicated jurisdictional disputes and slow extradition protocols. Perpetrators of such crimes, often, hide their identities by bouncing their communications in decentralized global servers and take the help of encryption strategies to protect their activities. This makes it difficult for investigators to find clues, as fragile digital evidence can be easily manipulated, damaged, or destroyed if the chain of custody is not carefully maintained. Many times law enforcement agencies lack specialized technical skills. Without appropriate access to forensic labs, technical training, and enough funding, it is difficult to decode complex digital networks, and even the best laws will struggle to lead to actual convictions.

[25] Information Technology Act, No. 21 of 2000 (India).
[26] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[27] Bharatiya Nyaya Sanhita, No. 45 of 2023 (India).

Additionally, this online landscape sees various changes over time. With the constant string of innovations in technologies like Generative AI, deep fakes, and Agentic AI, cyber laws can quickly become outdated. Going forward, India needs to shift from a reactive approach, which punishes offenders only after harm is done, to proactively creating a strong digital environment. This will require a cooperative, multi-faceted effort. We need up to date laws, as well as, specialized training for both police and judiciary in these domains. Spreading digital literacy amongst citizens and formalizing strong, real-time transnational cooperation treaties should be prioritized. Eventually, the aim is to keep individual citizens safe and uphold the nation's digital frontier during this unpredictable digital era.